ABSTRACT

A new method and apparatus for speeding up cryptographic calculations relies on faster methods for automatically calculating the solutions of certain equations. This includes a faster method for modular division, and a faster method for solving quadratic equations in characteristic 2 fields. The improvement speeds up key exchange, encryption, and digital signatures.